Microsoft Identity and Access Strategy

Microsoft Identity and Access Strategy

Situation

- Password fatigue
- Fraud, theft, phishing, pharming
- Heightened sensitivity to privacy, tracking
- Identity recognized by CxO as top business problem
- Demand for federated applications

“Laws of Identity”

1. **Control:** only reveal information identifying user with user’s consent
2. **Minimal disclosure:** solution disclosing least identifying information is most stable long term
3. **Fewest parties:** disclosure limited to parties having necessary and justifiable place in a relationship
4. **Directed identity:** must support omnidirectional and unidirectional identifiers
5. **Pluralism:** must support and channel multiple technologies run by multiple providers
6. **Human integration:** human user is component of distributed system integrated through unambiguous and safe communications mechanisms
7. **Contexts:** facilitate negotiation of mechanism between relying party and user of specific identity, while presenting consistent human and technical interface

Federated Identity Approach

- Meta-system
  - Embrace already deployed mechanisms
  - Allow evolution
- Claims-based model
  - *Claims* delivered in *security tokens* from *claims providers* to *relying parties*
- Be open with the industry
  - Use open protocols
  - Make implementation notes freely available

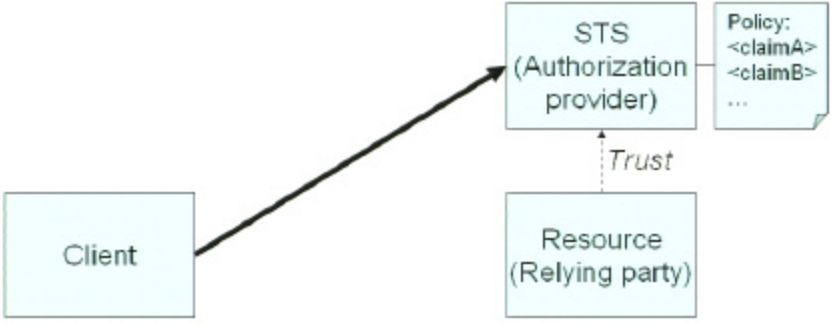
Claims

- Cryptographically verifiable information about one digital actor which another actor claims to be true
  - More than just identity assertions
- Claims transformation
  - At organizational or technical boundaries, one set of claims can be transformed into another
- Relying party specifies claims required and candidate claim providers
  - Authentication and authorization through single mechanism
- Claims delivered in security tokens (e.g. SAML) generated by Security Token Servers (STS)

Claims in WS-* Architecture

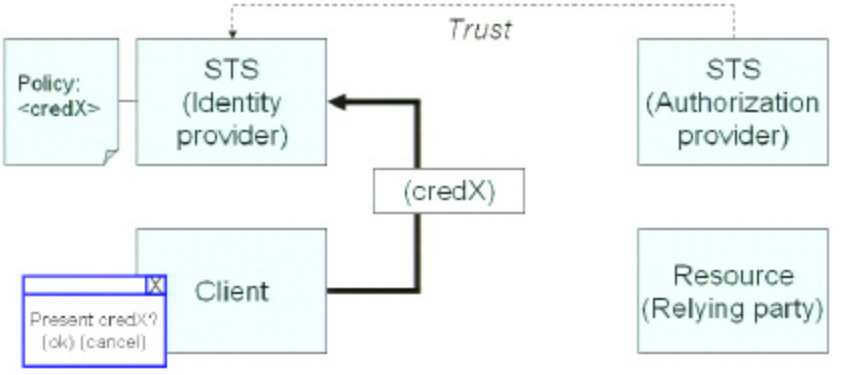
- Client to perform operation X at resource
- Client reads metadata associated with operation including policy
  - Policy indicates required claims, candidate claim providers necessary to perform operation
  - WS-MetadataExchange, WS-Policy, WS-SecurityPolicy

Claims in WS-* Architecture



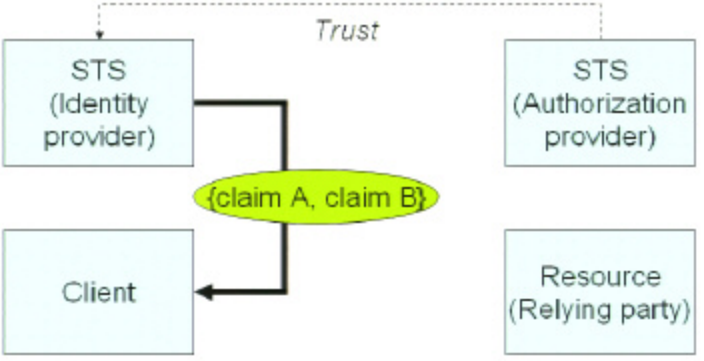
- Client requests security token with required claims from STS
  - WS-Trust
- STS policy indicates
  - Credentials necessary to obtain security token, or
  - Required claims, candidate claim providers to obtain security token

Claims in WS-* Architecture



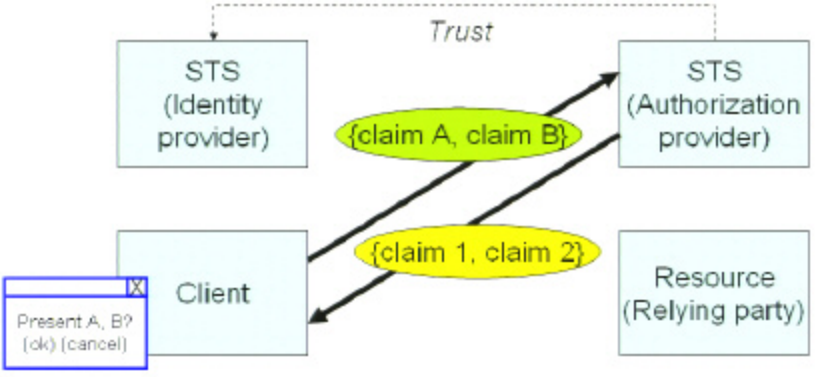
- Client requests security token from STS
- STS policy indicates credentials to obtain security token
- End user approves release of credential
- Client presents credential

Claims in WS-* Architecture



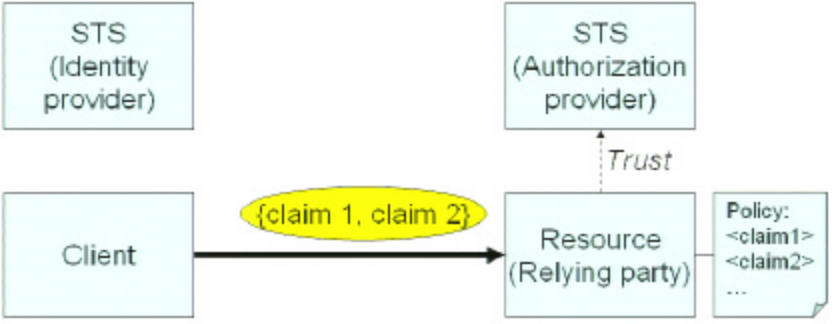
- STS returns security token

Claims in WS-* Architecture



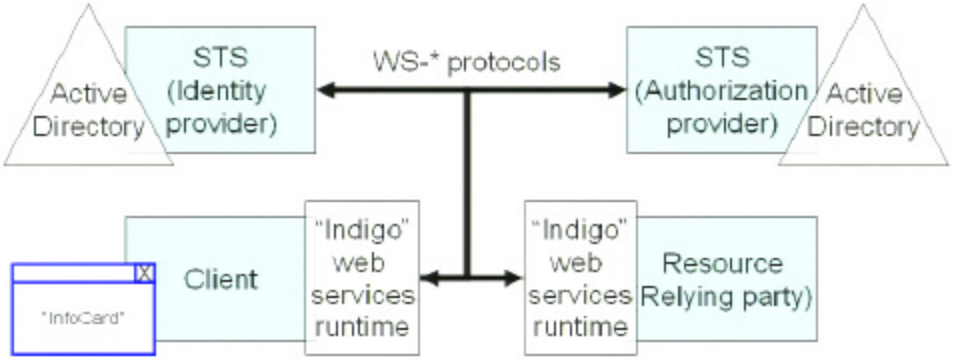
- End user approves release of claims
- Client presents security token to STS
- STS translates claims, returns security token

Claims in WS-* Architecture



- Client presents security token to resource

Microsoft Product Offering



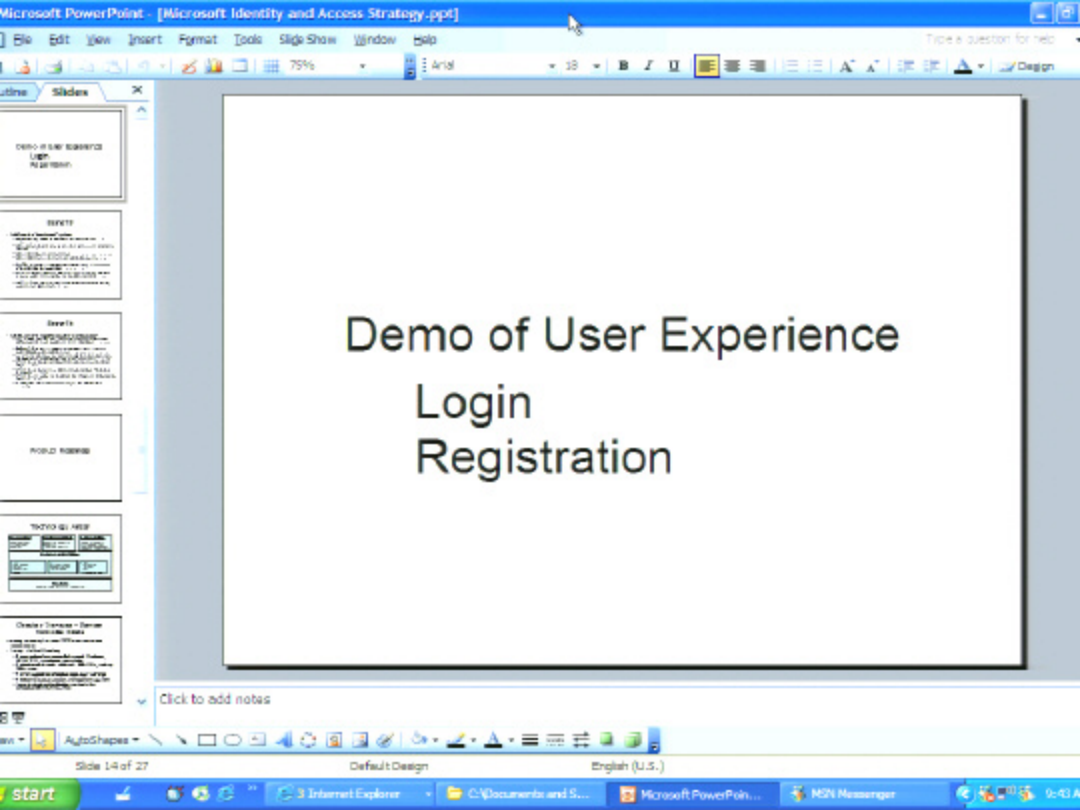
- Active Directory-integrated Security Token Services
- "InfoCard" end user experience
- "Indigo" web services runtime for application developers
- WS-* open, interoperable protocols

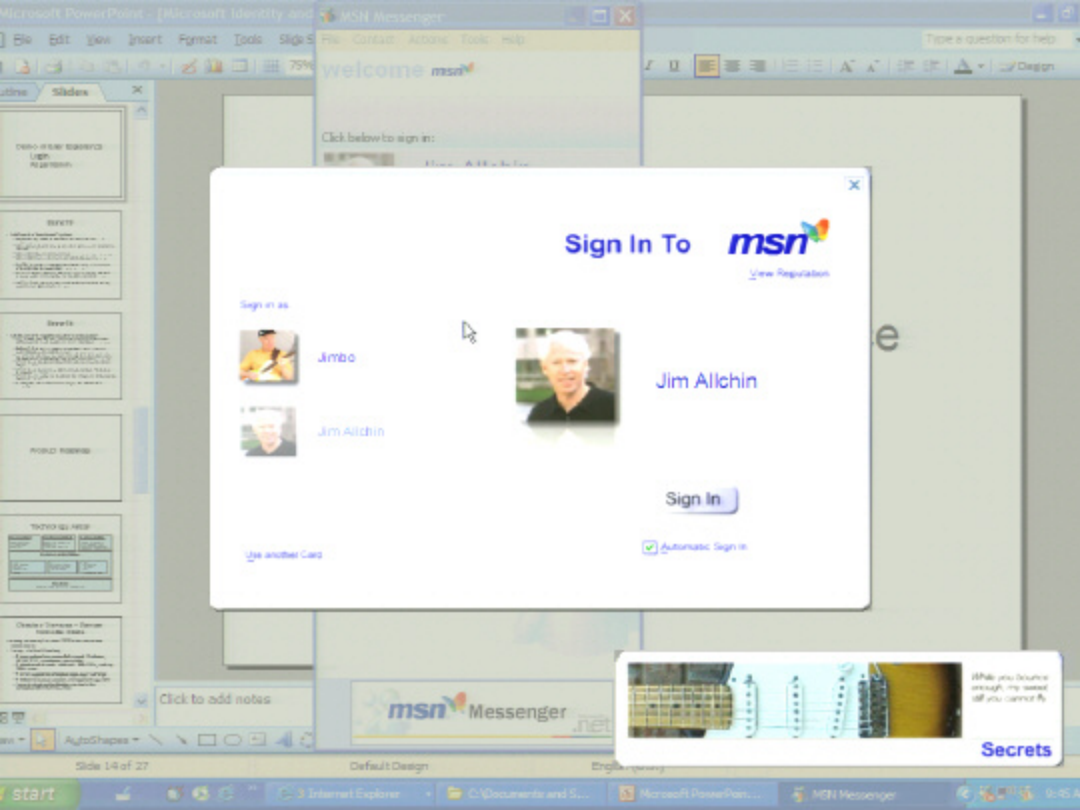
“InfoCard”

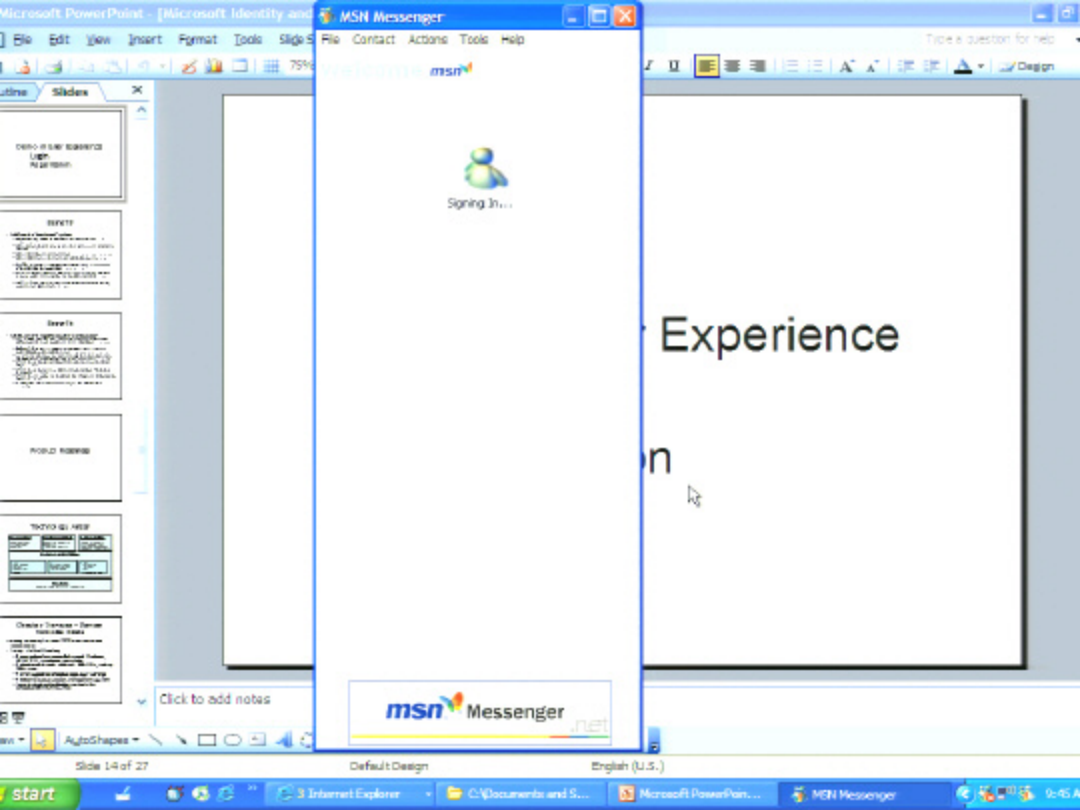
- Simple user abstraction
  - For managing collections of claims: identity claims, membership claims, possession claims, …
  - For managing keys for sign-in: strong computer generated keys instead of human generated passwords
- Grounded in real-world metaphor of physical cards
  - Gov’t ID card, driver’s license, credit card, membership card, …
- Support both self-issued and managed cards
  - Self-issued cards signed by user
  - Managed cards signed by external authority
- Implemented as secure subsystem
  - Protected UI, anti-spoofing techniques, encrypted storage

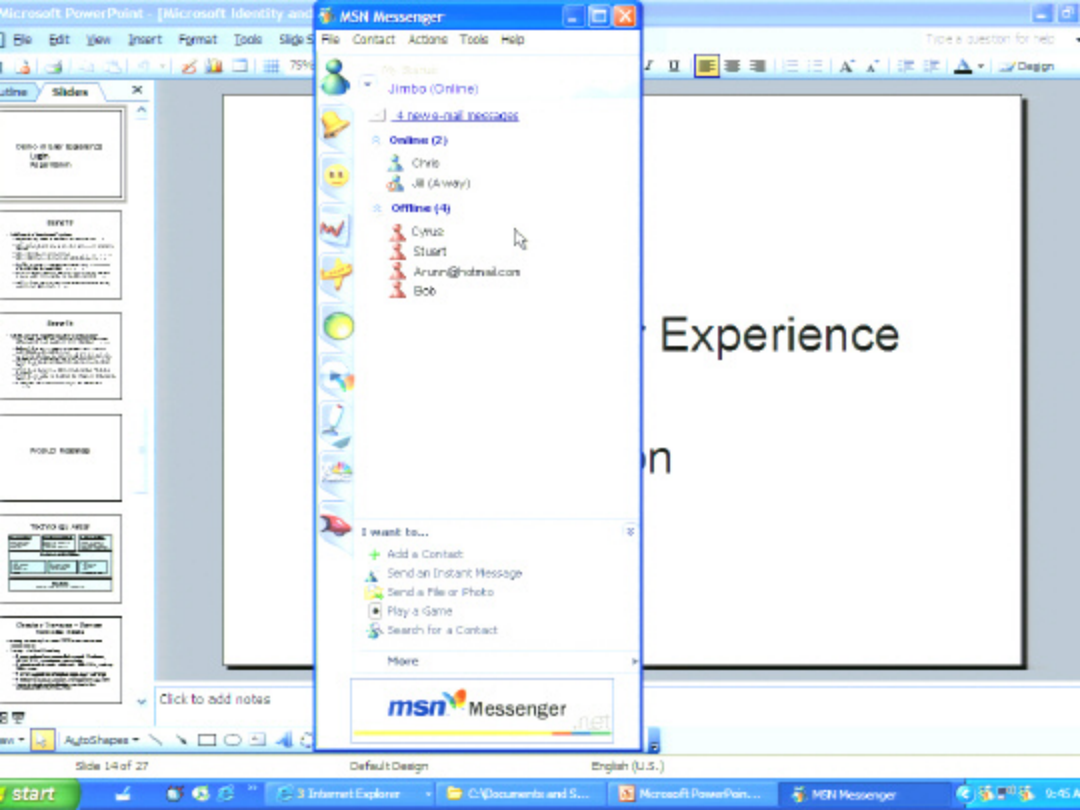
Demo of User Experience

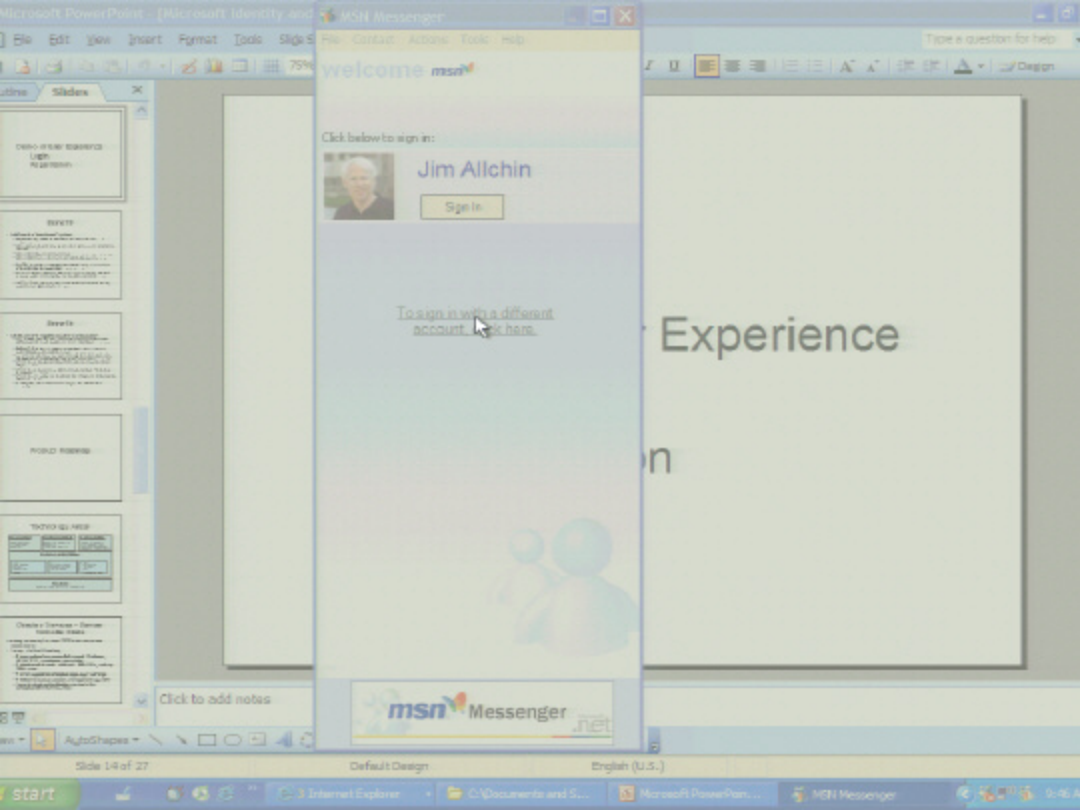
- Login
- Registration

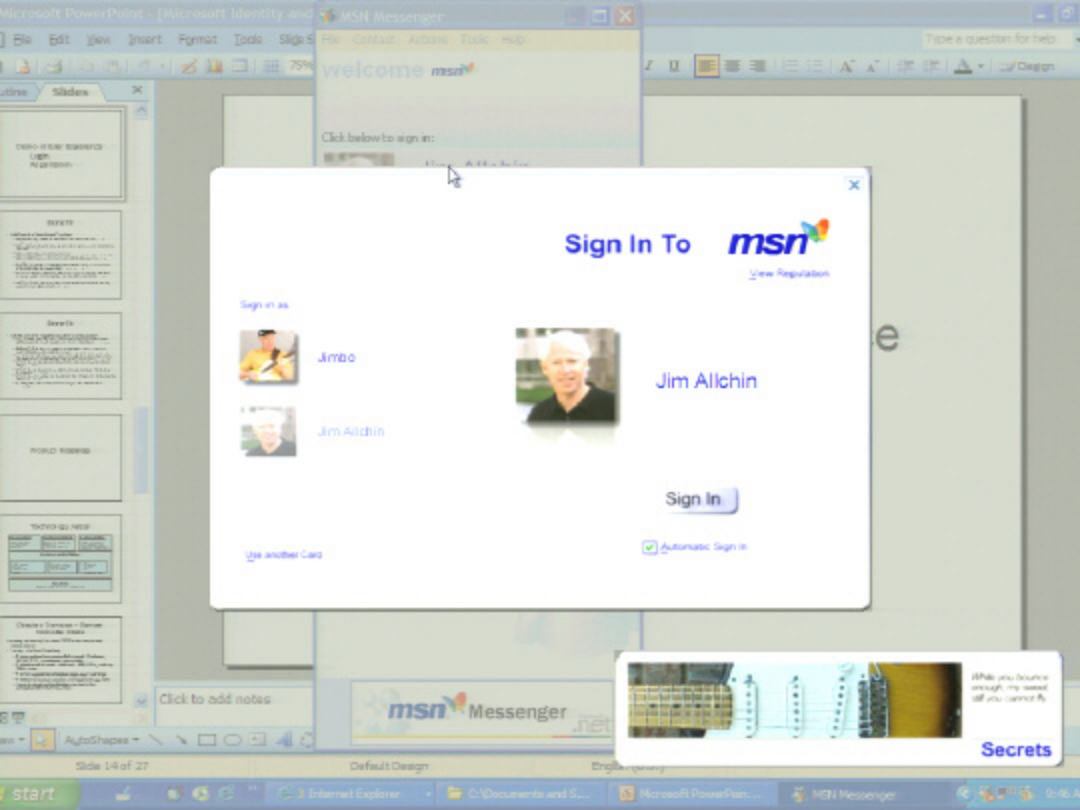

Microsoft PowerPoint - [Microsoft Identity and Access Strategy.ppt]
File Edit View Insert Format Tools Slide Show Window Help
Type a question for help
Arial
Design
Outline
Slides
Demo of User Experience
Login
Registration
Click to add notes
AutoShapes
Slide 14 of 27
Default Design
English (U.S.)
start
3 Internet Explorer
C:\Documents and S...
Microsoft PowerPoin...
MSN Messenger
9:43 A

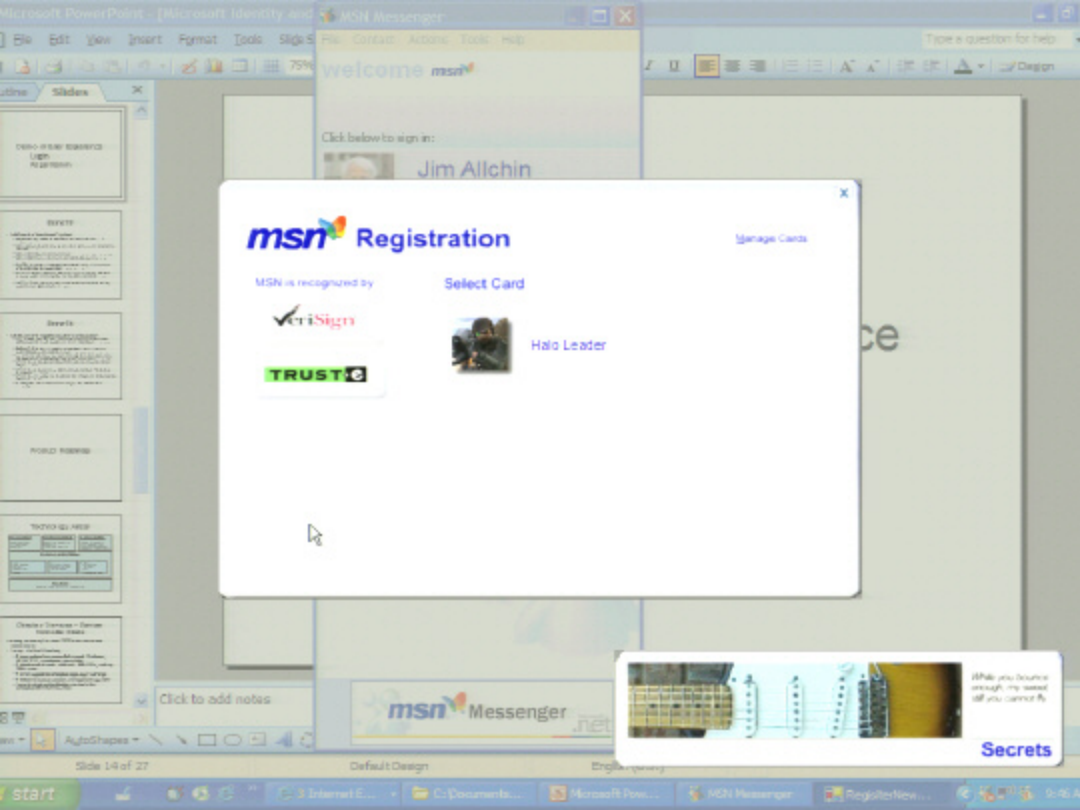

Sign In To msn
View Reputation
Sign in as
Jimbo
Jim Allchin
Jim Allchin
Sign In
Use another Card
Automatic Sign in
Secrets

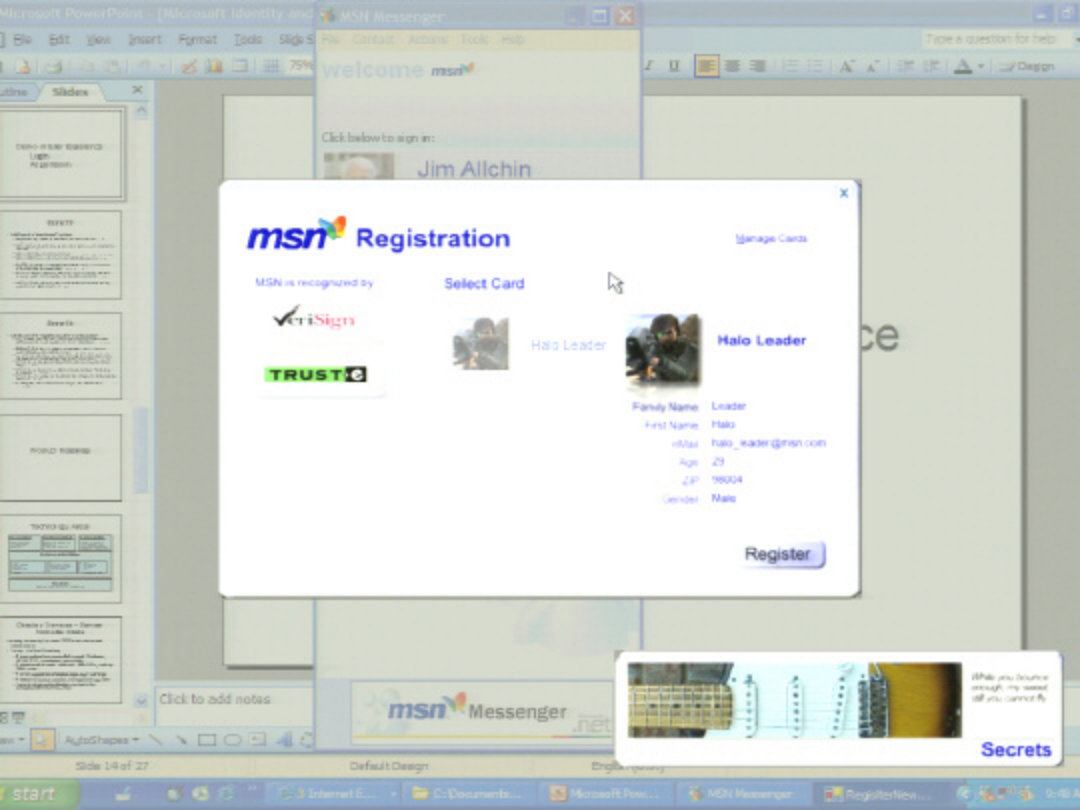

MSN Messenger
File Contact Actions Tools Help
msn
Signing In...
msn Messenger
.net
Experience
Click to add notes
Slide 14 of 27
Default Design
English (U.S.)
start
MSN Messenger


Microsoft PowerPoint - [Microsoft Identity and
File Edit View Insert Format Tools Slide S
Type a question for help
Design
Outline Slides
MSN Messenger
File Contact Actions Tools Help
Jimbo (Online)
4 new e-mail messages
Online (2)
Chris
Jill (Away)
Offline (4)
Cyrus
Stuart
Arunn@hotmail.com
Bob
I want to...
Add a Contact
Send an Instant Message
Send a File or Photo
Play a Game
Search for a Contact
More
msn Messenger
Experience
n
Click to add notes
AutoShapes
Slide 14 of 27
Default Design
English (U.S.)
start
Internet Explorer
C:\Documents and S...
Microsoft PowerPoint...
MSN Messenger


Microsoft PowerPoint - [Microsoft Identity and
File Edit View Insert Format Tools Slide S
Type a question for help
Outline Slides
MSN Messenger
File Contact Actions Tools Help
welcome msn
Click below to sign in:
Jim Allchin
Sign In
To sign in with a different account, click here.
Experience
n
Click to add notes
msn Messenger .net
AutoShapes
Slide 14 of 27
Default Design
English (U.S.)
start
3 Internet Explorer
C:\Documents and S...
Microsoft PowerPoint...
MSN Messenger

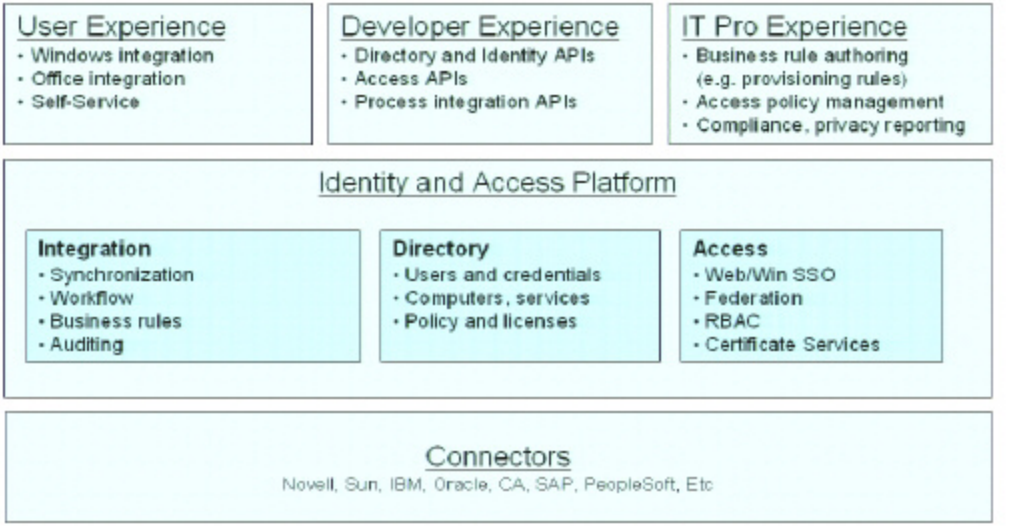

Sign In To msn
View Regulation
Sign in as:
Jimbo
Jim Allchin
Jim Allchin
Sign In
Use another Card
Automatic Sign in
Secrets


Microsoft PowerPoint - [Microsoft Identity and
File Edit View Insert Format Tools
MSN Messenger
File Contact Actions Tools Help
welcome msn
Click below to sign in:
Jim Allchin
msn Registration
Manage Cards
MSN is recognized by
VeriSign
TRUSTe
Select Card
Halo Leader
Click to add notes
msn Messenger
Secrets
Slide 14 of 27
Default Design
start

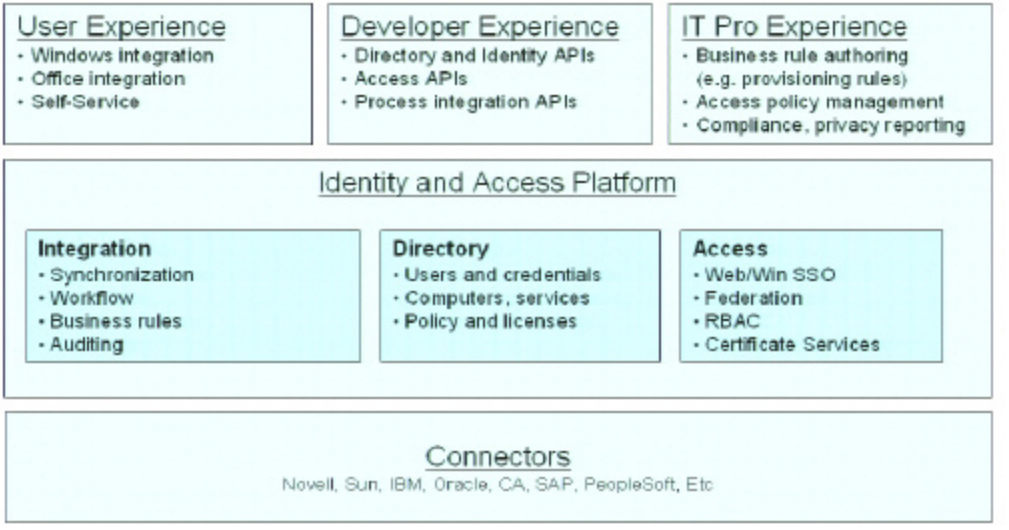

msn Registration
Manage Cards
MSN is recognized by
VeriSign
TRUSTe
Select Card
Halo Leader
Halo Leader
Family Name Leader
First Name Halo
eMail halo_leader@msn.com
Age 29
ZIP 98004
Gender Male
Register
Jim Allchin
msn Messenger
Secrets
Click to add notes

Product Roadmap

Technology Areas



Technology Areas

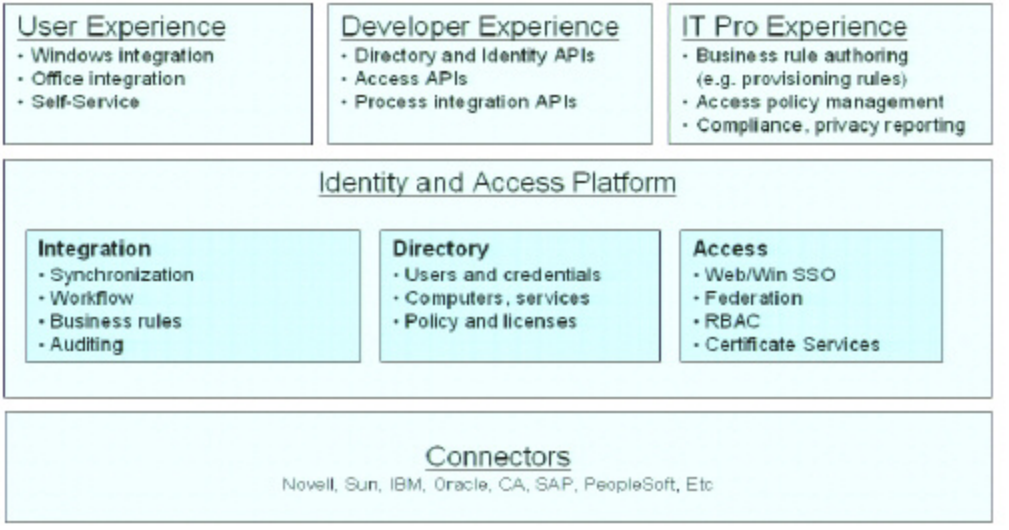


Product Roadmap

Demo of User Experience

- Login
- Registration

Technology Areas



Directory Services – Domain Controller Mode

Leading directory for host SSO and enterprise applications

- Today: Active Directory
  - Broad protocol and credential support: Kerberos, NTLM, SSL, smartcards, passwords
  - Performance at scale: scale out 1000+ DCs, scale up 20M+ users
  - Proven support for enterprise apps e.g. Exchange
  - Platform for secure systems management e.g. SMS
  - Trend to single authentication service in the enterprise for Unix/Linux, Mac

Directory Services – Domain Controller Mode (cont'd)

- R2
  - Unix compatibility schema
- Longhorn
  - Read-only DC: reduced physical security requirements, simplified manageability
  - Restartable AD: reduce domain controller reboots
  - DC on Server Foundation: minimize surface area
  - DC/Domain admin separation: simplified manageability

Directory Services – App Directory Mode

Flexibility in deployment for application developers and administrators

- Today: ADAM web download
  - LDAP-only mode of AD, virtually identical code as DC mode
  - Identical performance at scale
  - Independent schema, topology, and can be sync'd with AD
  - Suitable as extranet directory, app-specific directory
  - Redistributed by multiple vendors: Oblix, OpenNetwork, etc
- R2: ADAM included in OS distribution
  - Built-in one-way AD-to-ADAM sync, eliminates need to deploy MIIS/IIFP for simple scenarios
- Longhorn: same as R2

Access Services

Integrating federated claims-based identity and access capability into Active Directory

- Today
  - Comprehensive PKI support in platform
  - Role-based access control via Authorization Manager
  - Proven partnerships in extranet access management
- R2: Active Directory Federation Services v1
  - Federated web SSO
  - Interop-tested WS-Federation Passive Requestor Profile
  - Integrated with Windows SSO
  - Claims-based access model using SAML assertions
  - Federated SharePoint
- Longhorn: ADFS v1.1, AD STS, InfoCard

Integration Services

Improve security and reduce operational costs by automating and delegating identity and access management tasks

- Today: Microsoft Identity Integration Server 2003 SP1
  - Automate provisioning and de-provisioning
  - Enforce consistency of data across systems
  - Password management
- R2 wave: MIIS 2003 SP2
  - Reach: RACF/ACF2/Top Secret, SAP, Peoplesoft
  - Self service password reset

Integration Services (cont'd)

- Longhorn wave: MIIS "Gemini"
  - Advanced workflow
  - Advanced auditing and reporting
  - Declarative policy
  - Computed memberships
    - Staff DLs, building DLs
  - Self-service platform and applications
    - "AutoGroup"

Questions and Feedback